Prof. Dr. Johannes Blömer
Nils Löken, Peter Günther

April 15th, 2016
submission due: April 26th, 2016: 11 a.m.

Cryptography - Provable Security

SS 2016

Handout 2

Exercises marked (*) or (**) will be checked by tutors.

Exercise 1 (4 points)**:**
(**) Prove or refute: Every private key encryption scheme for which the size of the key space equals the size of the message space, and for which the key is chosen uniformly at random from the key space, is perfectly secret.

Exercise 2:
Let $l \in \mathbb{N}$ be arbitrary. Consider the one-time-pad encryption scheme Π with $\mathcal{P} = \mathcal{K} = \mathcal{C} = \{0,1\}^l$. When using this scheme with key $k = 0^l$, it follows from the construction that $\mathrm{Enc}_k(m) = m$ and the message is sent in the clear! It has therefore been suggested to improve the one-time-pad by only encrypting with a key $k \neq 0^l$. That is, the key is chosen uniformly at random from $\mathcal{K}' = \mathcal{K} \setminus \{0^l\}$ instead of $\mathcal{K}$. Is this really an improvement? In particular:

- Is the modified scheme Π' still perfectly secret? Prove your answer!
- Let $m, c \in \{0,1\}^l$, $m \neq c$ such that

  $$\Pr[\mathcal{P} = m] = p, \qquad \Pr[\mathcal{C} = c] = q,$$

  for some $0 < p, q < 1$. Compute the probability $\Pr[\mathcal{P} = m \,|\, \mathcal{C} = c]$.

Exercise 3 (4 points)**:**
(**) The key length in the one-time-pad encryption scheme is equal to the message length. Since short keys are desired, the following modification Π' of one-time-pad has been suggested:

$\Pi' = (\mathrm{Gen}', \mathrm{Enc}', \mathrm{Dec}')$ with $\mathcal{P} = \mathcal{C} = \{0,1\}^{2 \cdot l}$ and $\mathcal{K} = \{0,1\}^l$ for some $l \in \mathbb{N}$ is as follows:

- Gen': chooses $k \in \mathcal{K}$ uniformly at random.
- Enc': $\mathrm{Enc}'_k(m) := m \oplus (k \| k)$.
- Dec': $\mathrm{Dec}'_k(c) := c \oplus (k \| k)$.

where $k \| k$ denotes the concatenation of the bit strings.

a) Prove that the introduced private key encryption scheme is correct.

b) Is the modified scheme still perfectly secret? Prove your answer!

Exercise 4 (4 points)**:**
(*) Which of the functions $f_i : \mathbb{N} \to \mathbb{N}$ defined by

$$f_1(n) := n^{-\log\log(n)}, \qquad f_2(n) := 2^{-(\log\log(n))^2}, \qquad f_3(n) := 2^{-\sqrt{\log(n)}}, \qquad f_4(n) := 2^{-\sqrt{n}}$$

are negligible? Prove your answers!

Exercise 5:
Let $\mu_1(n), \mu_2(n)$ be negligible functions and $p(n)$ be a polynomial. Show that

- The function μ_3 defined by $\mu_3(n) := \mu_1(n) + \mu_2(n)$ is negligible.
- The function μ_4 defined by $\mu_4(n) := \mu_1(n) \cdot p(n)$ is negligible.

Exercise 6:
Consider Theorem 1.4. In the lecture you have proven that a private key encryption scheme $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ with message space $\mathcal{P}$, key space $\mathcal{K}$, ciphertext space $\mathcal{C}$ with

$$\Pr[\mathrm{Enc}_{\mathcal{K}}(m_0) = c] = \Pr[\mathrm{Enc}_{\mathcal{K}}(m_1) = c] \tag{1}$$

for all $m_0, m_1 \in \mathcal{P}$ and all $c \in \mathcal{C}$ is perfectly secret. Now, prove that every perfectly secret encryption scheme satisfies (1) for all $m_0, m_1 \in \mathcal{P}$ and all $c \in \mathcal{C}$.

Exercise 7 (4 points)**:**
(**) Let Π be any encryption scheme with a message space $\mathcal{P}$ that contains messages $p_1, p_2 \in \mathcal{P}$ of different length $|p_1| \neq |p_2|$.
Suppose that in the definition of indistinguishable encryption we do not require that the two challenge messages m_0, m_1 are of the same length. Show that in the sense of this definition, Π is not an encryption scheme with indistinguishable encryption. **Hint:** Let $q(n)$ be a (polynomial) upper bound on the encryption length of bit 0. Consider an adversary A outputs $m_0 = 0$ and a random $m_1 \in \{0,1\}^{q(n)+2}$.

Exercise 8 (4 points)**:**
(*) Consider the following alternative definition of indistinguishable encryptions. For $\beta \in \{0,1\}$ denote by $\mathrm{PrivK}^{eav}_{\mathcal{A},\Pi}(n,\beta)$ the indistinguishable experiment $\mathrm{PrivK}^{eav}_{\mathcal{A},\Pi}(n)$, except that the choice for the bit b in step 2 is fixed to the value β. Furthermore, denote the output b' of $\mathcal{A}$ in $\mathrm{PrivK}^{eav}_{\mathcal{A},\Pi}(n,\beta)$ by $\mathrm{output}(\mathrm{PrivK}^{eav}_{\mathcal{A},\Pi}(n,\beta))$. A private key encryption scheme $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ has indistinguishable encryptions if for every probabilistic polynomial time algorithm $\mathcal{A}$ there exists a negligible function $\mathrm{negl}(n)$ such that

$$\left|\Pr[\mathrm{output}(\mathrm{PrivK}^{eav}_{\mathcal{A},\Pi}(n,0)) = 1] - \Pr[\mathrm{output}(\mathrm{PrivK}^{eav}_{\mathcal{A},\Pi}(n,1)) = 1]\right| \leq \mathrm{negl}(n),$$

where k is distributed according to $\mathrm{Gen}(1^n)$ and the probabilities are with respect to the choice of k and the random choices of $\mathcal{A}$.
Show that this definition is equivalent to the definition of indistinguishable encryptions given in the lecture.

Exercise 9 (4 points)**:**
(**) Let $l : \mathbb{N} \to \mathbb{N}$ be a polynomial with $l(n) > n$ and let G be a deterministic polynomial-time algorithm such that for every $x \in \{0,1\}^n$ algorithm G outputs a string of length $l(n)$. We call G an almost-random generator if for every ppt algorithm $\mathcal{A}$ there exists a negligible function μ such that $\mathcal{A}$ wins the following game $\mathrm{Guess}_{\mathcal{A},G}(n)$ with probability at most $\frac{1}{2}+\mu(n)$.

Distribution guessing game $\mathrm{Guess}_{\mathcal{A},G}(n)$

- A bit $b \leftarrow \{0,1\}$ is chosen uniformly at random.
- If $b = 1$, then choose $x \leftarrow \{0,1\}^{l(n)}$ uniformly at random. If $b = 0$, then choose $s \leftarrow \{0,1\}^n$ and compute $x := G(s)$. The string x is given to $\mathcal{A}$.
- $\mathcal{A}$ outputs a bit $b' \leftarrow \mathcal{A}(1^n, x)$.
- $\mathcal{A}$ wins the game if and only if $b = b'$.

Show that an algorithms G is an almost-random generator if and only if it is a pseudorandom generator.